

8300 Greensboro Dr.
Suite 1200
McLean, VA 22102
WWW.FCCLAW.COM

Pamela L. Gist
(703) 584-8665
pgist@fcclaw.com

LNGS | LUKAS,
NACE,
GUTIERREZ
& SACHS, LLP

January 29, 2016

Marlene H. Dortch, Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C. 20554

Re: EB Docket No. 06-36
Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2015

Bluegrass Cellular, Inc.
Kentucky RSA #3 Cellular General Partnership
Kentucky RSA 4 Cellular General Partnership
Cumberland Cellular Partnership
Bluegrass Wireless LLC

Dear Ms. Dortch:

On behalf of Bluegrass Cellular, Inc. and its affiliates, and pursuant to Section 64.2009(e) of FCC rules, submitted herewith is the carriers' joint CPNI certification with accompanying statement covering calendar year 2015.

Should any questions arise regarding this submission, please contact the undersigned.

Very truly yours,



Pamela L. Gist

Enclosure

cc: Best Copy and Printing, Inc.

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 06-36**

Annual 64.2009(e) CPNI Certification for 2015

Date filed: January 29, 2016

Name of companies covered by this certification:

Bluegrass Cellular, Inc.

For and on behalf of

Kentucky RSA #3 Cellular General Partnership
499 Filer ID 802218

Kentucky RSA 4 Cellular General Partnership
499 Filer ID 802215

Cumberland Cellular Partnership
499 Filer ID 802221

Bluegrass Wireless LLC
499 Filer ID 825310

Address: P.O. Box 5012
Elizabethtown, Kentucky 42702

Name of signing officer: Ronald R. Smith

Title of signatory: President

CERTIFICATION

I, Ronald R. Smith, hereby certify that I am an officer of the companies named above, and acting as an agent of the companies, that I have personal knowledge that the companies have established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the rules of the Federal Communications Commission.

Attached to this certification is an accompanying statement which (i) explains how the companies' procedures ensure that the companies are in compliance with the requirements set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the Commission's rules, (ii) explains any action taken against data brokers during the past year, (iii) reports information known to the companies regarding tactics pretexters may be using to attempt access to CPNI, and (iv) summarizes any customer complaints received in the past year concerning the unauthorized release of CPNI.

The companies represent and warrant that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The companies also acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.



Name: Ronald R. Smith, President

Title: *President & CEO*

Date: *1-21-16*

Attachment: Accompanying Statement explaining CPNI procedures

Company Names (Collectively referred to as "Carrier"):

Bluegrass Cellular, Inc.

For and on behalf of

Kentucky RSA #3 Cellular General Partnership

Kentucky RSA 4 Cellular General Partnership

Cumberland Cellular Partnership

Bluegrass Wireless LLC

STATEMENT

Carrier has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Carrier has adopted a manual and keeps it updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.
- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Carrier's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.
- Carrier has implemented procedures to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier's retail locations or otherwise and in connection with these procedures, Carrier has established a system of passwords and back-up authentication methods which complies with the requirements of applicable Commission rules.
- Carrier has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.
- Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.
- Carrier took the following actions against data brokers in 2015, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission:
 - No instances of CPNI violations stemming from data brokers, no action taken
- The following is information Carrier has with respect to the processes pretexters are using to attempt to access CPNI, and [if any] what steps carriers are taking to protect CPNI:
 - Call Center: Persons calling stating that they are the account holder when they are not – Verification of personal information prior to discussing the account information is used to protect CPNI. Detail call records are only mailed to the account billing address (never faxed or sent to another address).

- Retail Location - Persons stating that they are the account holder when they are not – Verification of picture id prior to discussing any account information or release of bills or call records.
- The following is a summary of all customer complaints received in 2015 regarding the unauthorized release of CPNI:

- Number of customer complaints Carrier received in 2015 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: 17

Category of complaint:

- 5 Number of instances of improper access by employees
- 11 Number of instances of improper disclosure to individuals not authorized to receive the information
- 0 Number of instances of improper access to online information by individuals not authorized to view the information
- 1 Number of other instances of improper access or disclosure

- Summary of customer complaints received in 2015 concerning the unauthorized release of CPNI:
 - 1/29/15: Customer alleged an agent staff member disclosed account information to customer's ex-girlfriend. CPNI Investigation was inconclusive.
 - 4/13/15: Customer alleged that detailed call records were requested by non-authorized user and mailed to her home. Call recordings indicated that the records request came from the account holder who is authorized to make such requests. Investigation confirms a CPNI violation did not occur
 - 5/6/15: Customer alleged that a non-authorized person obtained his call logs from a staff member. Investigation confirms that a CPNI violation did occur.
 - 5/11/15: Customer alleged that a staff member was disclosing account information to his cousin. Investigation confirms that a CPNI violation did not take place.
 - 6/23/15: Customer alleged that a staff member used improper access to her account to send obscene messages to her. A CPNI investigation concluded that a violation did not take place.
 - 6/26/15: Customer alleged that a staff member was disclosing account information to her ex-husband. A CPNI investigation concluded that a violation did not occur.
 - 9/4/15: Customer requested that a staff member be restricted from viewing information on her account. Our CPNI investigation confirmed that the employee was accessing the account information improperly and that the violation did occur. The employee resigned.
 - 9/16/15: Customer complained that someone who obtained his traded-in device had access to the customer's text messages and account information. Our CPNI investigation confirmed that the device was not properly processed by an agent staff member and the CPNI violation did occur.
 - 9/21/15: Customer alleged that an agent staff member improperly accessed their account to process a device change for an unauthorized person. A CPNI investigation confirmed that this occurred.

- 10/6/15: Customer alleged that a staff member was disclosing their phone number to various persons including his ex-girlfriend. A CPNI investigation concluded that this did not occur.
- 10/14/15: Customer alleged that a staff member was disclosing account information to a particular person. Our CPNI investigation concluded that this did not occur.
- 10/19/15: Customer alleged that her brother's text messages were obtained by an unauthorized person as they were presented in court during his trial. A CPNI investigation determined that the records were obtained via court order so a CPNI violation did not occur.
- 10/27/15: Authorized user alleged that a staff member was disclosing call records from her account. A CPNI investigation concluded that the violation did not occur.
- 11/16/15 - Customer alleged that a staff member was disclosing account information. A CPNI investigation concluded that a CPNI violation did not occur.
- 12/9/15: Customer alleged that an agent staff member accessed her account improperly to make changes. A CPNI investigation concluded that this violation did occur.
- 12/28/15: Customer alleged that a staff member accessed her account improperly to make changes. A CPNI investigation concluded that this violation did occur. The staff member's employment was terminated.
- 12/29/15: Customer alleged that an agent staff member disclosed account information to an unauthorized person. CPNI investigation concluded that the violation did occur.